Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 10, Issue 1; January-March, 2023, pp. 6-19

http://www.krishisanskriti.org/Publication.html

# Exploring the Security Challenges in the Cloud Enabled IoMT Sector and Promising Solutions Ahead

**Md. Afroz[1] and Birendra Goswami[2]**

*[1,2]Department of Computer Science & IT Sai Nath University, Ranchi, Jharkhand, India*
*E-mail: [1]afrozhasnain@gmail.com, [2]bg.ranchi@gmail.com*

**Abstract—***The advent of IoT devices has ushered in a new era of connectivity, permeating various facets of contemporary life. This pervasive integration of technology has engendered a future teeming with possibilities, promising manifold benefits for individuals, information management, and operational processes. As individuals find themselves equipped with an increasing amount of leisure time, they are afforded the opportunity to orchestrate comprehensive life cycles that encompass both personal and professional spheres of influence. Notably, the Internet of Medical Things (IoMT) has emerged as a thriving domain, providing hospitals and clinicians with access to sensitive information pertaining to human lives. However, this proliferation of interconnectedness also introduces a concomitant risk—a fertile ground for malicious actors seeking to exploit vulnerabilities inherent in the IoMT infrastructure.*

*In light of these circumstances, the establishment of uniform rules and foolproof methodologies becomes imperative. Although numerous organizations have undertaken the task of creating standards, the prevailing system still exhibits openings that expose the product to potential risks. The IoMT network, while boasting several well-established procedures, encounters hindrances to widespread adoption due to a range of issues. One prominent challenge lies in the composition of IoMT networks, which often comprise battery-operated devices characterized by limited processing capacity. This inherent constraint poses a significant hurdle in the path toward achieving widespread adoption and necessitates innovative solutions to address this predicament.*

*Extensive literature provides an overview of IoT security integrations, and within this context, this article aims to present a concise summary of the IoMT ecosystem. It delves into pertinent aspects such as legislation, challenges surrounding the establishment of standards, and various security measures utilizing cryptographic solutions, PUF-based approaches, blockchain technology, and named data networking (NDN). Through a meticulous analysis of each solution, this article aims to shed light on their respective advantages and downsides, facilitating informed decision-making and fostering a deeper understanding of the intricacies involved.*

*By examining the legislative landscape surrounding IoMT, stakeholders can gain insights into the regulatory frameworks governing the secure deployment of interconnected medical devices. Furthermore, understanding the challenges impeding the establishment of standardized protocols provides valuable perspectives on the current state of IoMT security. Investigating cryptographic solutions, such as encryption algorithms and secure key management, offers a glimpse into how data protection can be fortified. Similarly, exploring PUF-based solutions, which leverage the inherent uniqueness of physical properties, unveils potential avenues to enhance security. The article also delves into the potential of blockchain technology, a decentralized and immutable ledger, and its role in bolstering IoMT security through enhanced data integrity and access control mechanisms. Lastly, the examination of named data networking (NDN) sheds light on its potential to address security concerns by prioritizing content-centric communication and facilitating secure data sharing.*

*While each security measure presents distinct advantages, such as data confidentiality, integrity, and availability, it is vital to consider the associated trade-offs and potential downsides. By critically evaluating these factors, stakeholders can make informed decisions when implementing IoMT security measures, mitigating risks and ensuring the protection of sensitive medical information.*

*In summary, the increasing accessibility and utilization of IoT devices, particularly within the realm of the IoMT, hold promise for a brighter future. However, it is imperative to address the challenges posed by vulnerabilities in the IoMT infrastructure through the establishment of uniform rules and robust security measures. This article provides a comprehensive overview of the IoMT ecosystem, elucidates the legislative landscape and challenges of standardization, and explores various security measures, allowing stakeholders to make informed decisions in navigating the complex realm of IoMT security.*

**Keywords***: IoMT, Internet of Medical Things; encryption; security and privacy, physical unclonable function*

## INTRODUCTION

Wireless technology and its associated advancements in wireless communications have become deeply ingrained in our daily lives, owing to the continuous progress in technology. Notably, the Internet of Things (IoT) has emerged as a pivotal driver of the ongoing internet revolution. The IoT facilitates the integration of real-world objects into computer systems, leveraging technological advancements to make this integration increasingly viable [1]. This transformative concept holds immense potential across various sectors, particularly in domains such as home automation and health monitoring [2]. The IoT functions as a network that connects physical objects through wireless networking protocols,

enabling the collection and distribution of data using smart healthcare devices and other "Things" [2]. By combining data processing and analytics, the IoT empowers the internet to glean insights and make informed judgments about real-world objects. An alternative term, the "Internet of Objects," is sometimes used to denote this concept. IoT devices encompass a wide range of electrical and electronic devices, each serving diverse purposes and exhibiting varying forms [3]. The applications of IoT span across numerous domains, including home automation, industry, healthcare, energy management, environmental monitoring, and communication systems [3].

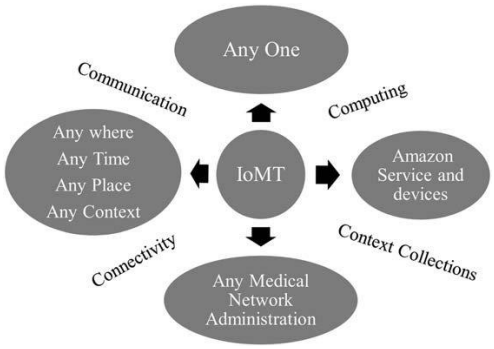


**Figure 1: IoMT threats**

The increasing interconnectivity of medical devices, facilitated by the IoT, holds significant implications for healthcare. For instance, it promises to enhance the detection and management of chronic illnesses, which is particularly valuable given the global aging population [4]. According to a study by Deloitte, the market is currently inundated with over half a million distinct medical technologies [5]. Within the realm of the IoT, wearable devices and medical/vital monitors are notable examples of Internet of Medical Things (IoMT) devices, designed for use in various settings such as homes, communities, clinics, and healthcare facilities [6]. These devices offer the potential for real-time location tracking, telemedicine services, and other healthcare-related functionalities [6].

The World Health Organization (WHO) defines e-health as the utilization of information and communication technology (ICT) in healthcare settings. Notably, within the field of e-health, there are subfields such as electronic health records (EHR), personal health records (PHR), and mobile health (m-Health), with IoT playing a prominent role in enabling their functionality [7]. Figure 1 illustrates the security concerns associated with IoMT. The IoT environment comprises data-gathering devices, internet connectivity, and software and hardware components responsible for data processing, protection, transmission, and visualization [8]. In practice, sensor data from implantable and wearable devices is transmitted to a cloud server via the internet or a gateway, where it is stored as patient health information (PHI) [6, 9]. Alongside wearables and clinical monitors, the IoMT industry encompasses telemedicine services, other applications, and real-time tracking functionalities [6]. The following sections outline the five key components of the IoMT ecosystem.

## EASE OF USE

### a) The On-Body Section

What is a Body Area Network (BAN)? A BAN is a network medium for transmitting patients' vital signs, which are measured by a wearable or a portable sensor. According to the research of Kocabas et al. [54], biological signals can be used to encrypt communications between medical equipment. Since this is an issue, Poon et al. [55] introduced a low-power bio-identification mechanism that uses an Inter-Pulse Interval (IPI) to encrypt the data exchanged by Body Area Network sensors. Using a secret key of the symmetric key cryptosystem and a physiological signal that agrees on it, Venkatasubramanian et al. [56] were able to communicate BAN sensors. Therefore, there are two methods by which the gathered medical data reaches the controller.

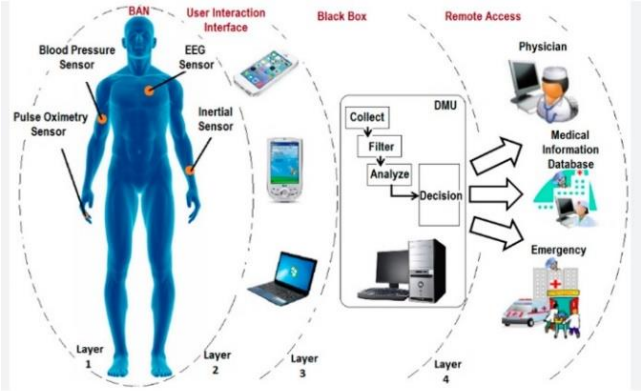


**Figure 2: The On-Body Section**

### b) In Home Section

In this scenario, the home uses sensor data to learn about its residents' health and habits. Mobile devices, display systems, and home robots are all provided to residents, and they are controlled by an autonomous system within the home. [11]. Telehealth services, remote patient monitoring, and personal emergency response systems make up this sector (TVV). The use of such technology paves the way for remote drug management, care for the elderly in the comfort of their own homes, and management of chronic diseases.

- Seniors and others who rely on them can use PERS's mobility devices (MDs) to stay put. This system combines a wearable gadget or relay unit with a 24/7 medical contact centre to ensure that help is always just a phone call away.
- RPM: This system uses continuous monitoring of physiological indicators to delay the progression of disease, shorten recovery times, and prevent readmission to the hospital. It includes all sensors and home monitoring systems that can alert users when it's time to take their medications and how much to take.

- Televisual (TVV): Digital testing and telemedicine are two examples of TVV. It enables people to avoid unnecessary hospitalizations by facilitating the acquisition of necessary medical care, including medicines and suggested treatment regimens.

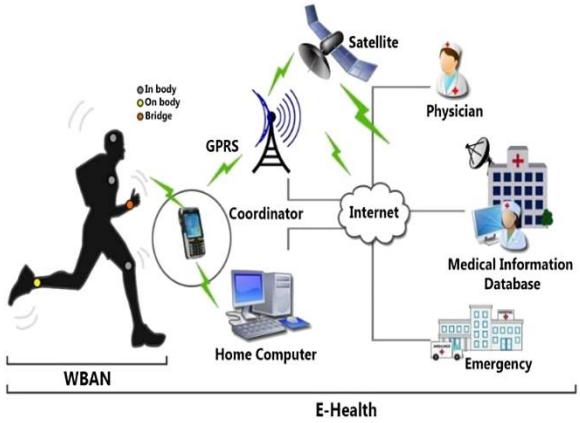


**Figure 3: In-Home Section**

### c) In-Community Section

In the communal part [12], we take local municipal doctors and radio stations into account. The five parts of this section are as follows:

- Portability: while in transportation, patients' vital signs are monitored by this service.
- First responders: Nurses, and doctors in hospitals' emergency rooms can all benefit from emergency response knowledge.
- Kiosks: these are self-service terminals that may sell goods or offer services like directing users to local healthcare providers.
- Point-of-care technology: physicians who provide care in venues other than hospitals, such as mobile clinics and health fairs.
- logistics : In the logistics industry, examples of equipment include pressure, temperature, humidity, shock, and tilt sensors for use in the transport of pharmaceuticals..

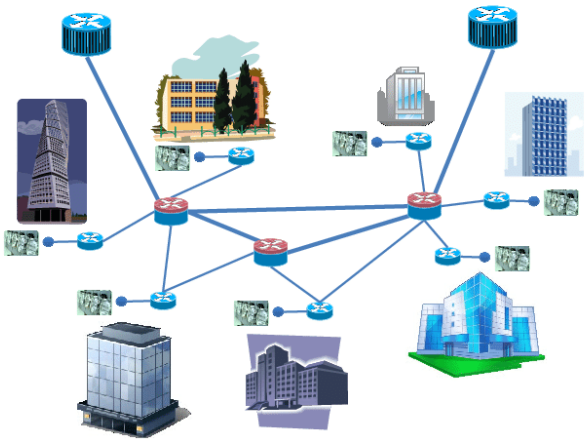

**Figure 4: In-Community Section**

### D. In-Clinic Section

Medical doctors aid in data collection and clinic operations by offering expert advice [6].

- Medical doctors who work in either an administrative or clinical capacity;
- Medical doctors with full-time employment in either an administrative or clinical capacity.
- In this field, qualified individuals can use a product while the service provider is located elsewhere.

### E. In- Hospital Section

This category includes IoMT-enabled equipment and solutions for hospital asset, personnel, patient flow, inventory, eenvironmental (temperature, pressure, and humidity), and energy monitoring. In this category [13] you'll find Zoll's wearable defibrillator and Stanley Healthcare's hand-hygiene compliance system.

Eavesdropping, data leak, DoS, physical attacks, cloning, side-channel attacks, remote hijacking, impersonation, password guessing, and man-in-the-middle (MITM) are all hostile threats. Physical attackers must be near the target device. If an attacker takes control of a device, they can clone it to access sensitive data. [16]. As an example of a side-channel assault, timing and power analysis can be used. In an eavesdropping attack, a hacker monitors a network and either steals information or manipulates it by intercepting, erasing, or modifying transmissions between two devices. An attacker can use a man-in-the-middle attack (MITM) to eavesdrop on a conversation between two IoT devices and steal their private information. DoS attacks are launched when a target's resources are blocked [17]. The IoMT network must be protected from intrusion if it is to remain operational.

From the foregoing, it is clear that IoMT is rapidly gaining importance, and a secure setting is necessary for its proper functioning and the protection of sensitive data. The remainder of the text follows the structure of

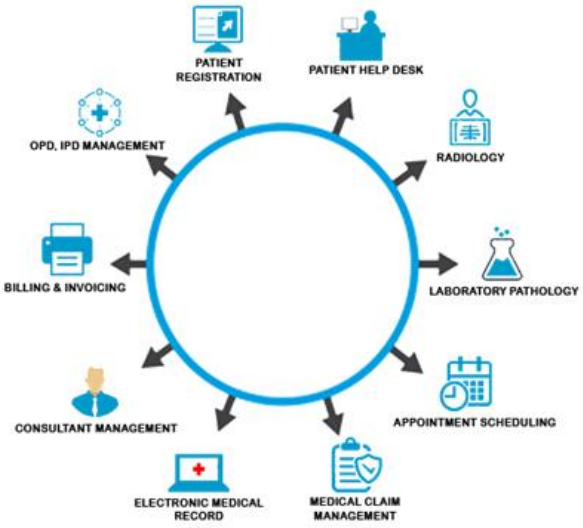


**Figure 5: In-Hospital Section.**

## LITERATURE REVIEW

IoMT (Internet of Medical Things) is a critical infrastructure closely tied to human safety and the protection of private data. To ensure its robustness, numerous tests are being conducted to determine the most effective methods for safeguarding the system. This survey study aims to provide a comprehensive and organized explanation of the IoMT system and recent research accomplishments, facilitating a comprehensive understanding of the field as a whole. Several authors have conducted surveys on IoMT, addressing various aspects of security and privacy. Sham-soshoara et al. [18] proposed security measures using Physically Unclonable Functions (PUF), while Fernández-Caramés et al. [19] highlighted the challenges of implementing security measures in the IoMT ecosystem. Alwarafy et al. [20] introduced intrusion detection techniques using edge computing, while Shakeel et al. [21] focused on small-scale security systems. Al-Garadi et al. [22], Arora et al. [23], and R. explored security and privacy risks in IoMT, discussing both centralized and decentralized solutions, as well as implementation issues and constraints.

The article under consideration discusses several key points related to IoMT security and privacy. Firstly, it delves into the IoMT network, device segmentation, and network threats, highlighting the significance of understanding these aspects in ensuring a secure environment. The article emphasizes the importance of the IoMT ecosystem in the modern world and its role in transforming healthcare practices. It also provides an overview of the laws governing medical devices and outlines the issues associated with their implementation.

Furthermore, the article explores security mechanisms commonly employed for devices with limited resources, considering their effectiveness in safeguarding IoMT systems. It thoroughly discusses the advantages and disadvantages of various proposed security frameworks, including centralized, decentralized, and Named Data Networking (NDN) approaches.

By addressing these key points, the article aims to provide a comprehensive understanding of IoMT security, privacy risks, and potential solutions. This in-depth analysis facilitates informed decision-making regarding the implementation of secure IoMT systems and contributes to the overall advancement of the field.

## THE IOMT ECOSYSTEM'S IMPACT ON HEALTHCARE

The utilization of IoMT (Internet of Medical Things) is experiencing rapid expansion on a daily basis. Particularly in the context of the COVID-19 pandemic, the promising characteristics of the IoMT ecosystem have been highlighted, leading to increased promotion and adoption. This section aims to discuss the role and functionality of the IoMT system, as well as the global growth and expansion of the IoMT market.

### III. I GLOBAL IOMT MARKET:

The global IoMT market is projected to grow at a Compound Annual Growth Rate (CAGR) of 18.5% from 2021 to 2027, with an anticipated market value of USD 284.5 billion by 2027. According to a study, connected Medical Devices (MDs) accounted for approximately 48% of all MDs in 2020, and this proportion is expected to rise to 68% by 2025. Furthermore, the year 2020 is predicted to witness the availability of 50,000 pharmaceuticals utilizing IoMT technology, leading to potential annual healthcare cost savings of approximately USD 300 billion. The research and development (R&D) expenditure on connected MDs is expected to increase from 34% in 2020 to 42% in 2025. Figure 3 illustrates the anticipated growth of the IoMT market, projecting a CAGR of 24.4% and reaching a market value of USD 254.2 billion by 2026. The smart wearable devices category is expected to dominate the market during the projected period, as indicated by All the Research.

These statistics reflect the substantial growth potential and increasing market demand for IoMT technologies. The proliferation of connected MDs and the integration of IoMT solutions are set to revolutionize healthcare practices and contribute to significant cost savings. The anticipated rise in R&D spending on connected MDs further underscores the industry's focus on innovation and advancement. As the IoMT market continues to expand, the dominance of smart wearable devices is expected, serving as a testament to the growing popularity of wearable technologies in healthcare settings.

In conclusion, the global IoMT market is experiencing remarkable growth, driven by factors such as increased adoption of connected MDs, advancements in pharmaceutical IoMT applications, and the potential for substantial cost savings in healthcare. The projected market growth and dominance of smart wearable devices highlight the expanding significance of IoMT technologies in revolutionizing healthcare delivery and improving patient outcomes.

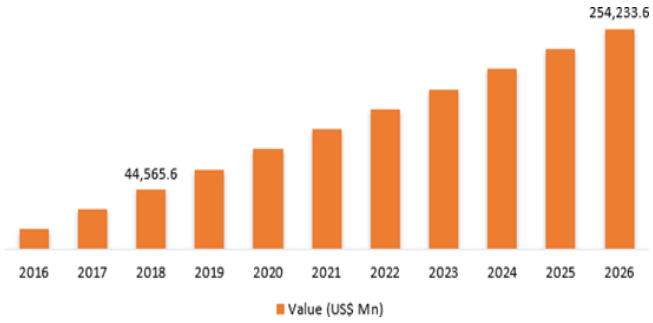


**Figure 6: Global Internet of Medical Things (IoMT) market from 2016 to 2026 in US dollars [28].**

The adoption of cloud data storage systems eliminates the need for users to store their data locally, as it is securely stored in the cloud. This approach ensures the safety, reliability, and accessibility of data files, as they are stored on distributed cloud servers [29]. The global IoMT market is expected to

witness substantial growth, with a projected value of USD 158.1 billion in 2022, a significant increase from USD 41 billion in 2017. In response to this growth, the industry's R&D budget allocation is expected to rise from the current 34% to 42% within the next five years [30].

The increase in healthcare spending is closely linked to the aging population, as by 2040, the elderly population is estimated to double, resulting in a rise in healthcare expenditure from USD 7.1 trillion in 2015 to USD 8.47 trillion in 2020 [5]. In order to address the challenges posed by this demographic shift and to optimize healthcare delivery, the future medical system is expected to heavily rely on IoMT technology. By leveraging IoMT, healthcare systems aim to reduce costs, minimize wait times, and improve treatment outcomes.

Figure 4 illustrates the projected growth of the global IoMT market up to 2030, emphasizing the potential for further expansion and adoption of IoMT technologies.

These statistics and projections highlight the increasing importance of IoMT in healthcare, as it offers a scalable and efficient solution for data storage, enhances healthcare services, and has the potential to drive significant cost savings.

The future medical landscape is expected to witness a comprehensive integration of IoMT to address the needs of an aging population and to optimize healthcare systems. The projected growth of the IoMT market underscores its potential to revolutionize healthcare practices and improve patient outcomes on a global scale.

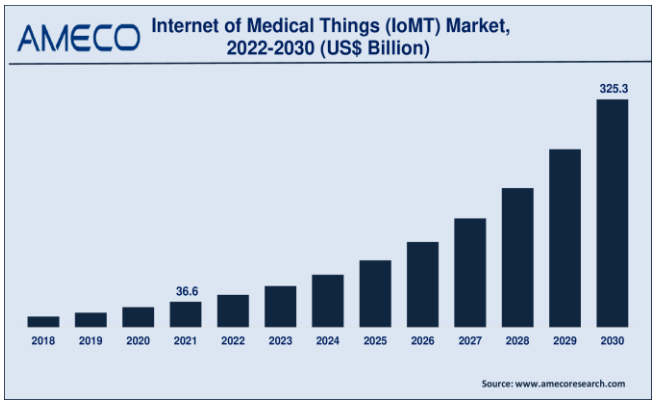


**Figure 7: Internet of Medical Things (IoMT) growth forecast for the world**

## III. II JUSTIFICATIONS FOR IOMT ADOPTION AND IMPLEMENTATION

According to the Deloitte report [30], the opportunity for remote patient monitoring, better patient care, and patient happiness are the primary enablers of IoMT adoption, as shown in Figure 5.


**Figure 8: The advantages of IoMT systems.**

Gus Vlahos, the director of healthcare sales for CDW in the Central Region, has identified five key factors contributing to the acceptability of IoMT in hospitals [31].

- Firstly, IoMT technology boosts and accelerates clinical workflows by providing conveniently small and portable devices. These instruments facilitate essential tasks such as SMS transmission, barcode scanning, and image transmission, improving the efficiency and effectiveness of healthcare processes.
- Secondly, IoMT promotes closeness between medical devices (MD) and healthcare professionals through automation and real-time alerts. Smart drugs and ultrasound machines can generate real-time alerts, enabling hospitals to promptly respond to critical situations.
- Thirdly, remote medical services play a crucial role in patient-doctor engagement and remote monitoring. Wi-Fi or Bluetooth-enabled devices, such as blood pressure cuffs, glucose meters, and heart rate monitors, allow patients to transmit their health data to doctors for analysis and appropriate treatment. Remote Patient Monitoring (RPM) has shown promising outcomes, enhancing medicine adherence and reducing costs in European hospitals.
- Fourthly, IoMT facilitates a proactive approach to maintaining health by utilizing consumer wearable devices. These devices enable the collection and transmission of patient health data to healthcare professionals, empowering them to provide necessary assessments and proactive care. Wearable devices, such as smartwatches and fitness bands, incorporate new types of sensors to monitor blood oxygen levels, track heart rate, and deliver alerts via SMS.
- Lastly, ensuring appropriate security measures is of paramount importance in the adoption of IoMT. Despite their numerous advantages, MDs are vulnerable to security risks due to network and device vulnerabilities, unfixed default passwords, and infrequent software

updates. It is essential to prioritize end-to-end security methods and reliable network monitoring to safeguard patient data and maintain the integrity of IoMT systems.

By considering these factors, hospitals can embrace IoMT technologies effectively, enhancing clinical workflows, patient care, and data security. The identification and implementation of these factors contribute to the successful integration of IoMT in healthcare settings, facilitating improved healthcare outcomes and patient experiences.

### III. III IOMT'S ROLES IN HEALTHCARE

The implementation of IoMT (Internet of Medical Things) has demonstrated several significant benefits, including lower error rates, improved accuracy in disease diagnosis, cost savings for healthcare organizations, and enhanced remote patient-doctor communication. These advantages have translated into substantial outcomes, such as savings of USD 2.5 million in a year, a 90% reduction in patient admission time, a 33% reduction in the length of stay for cardiac resynchronization treatment, a 37% reduction in procedure cancellations due to improved patient planning and scheduling, and a 43% reduction in staff overtime. These achievements highlight the positive impact of IoMT on healthcare operations and patient outcomes.

Moreover, IoMT technologies have been effectively employed in conjunction with other measures to mitigate the transmission of COVID-19, which is particularly crucial during the ongoing outbreak. IoMT serves as a protective barrier for front-line workers, boosting productivity while minimizing the impact of the disease on people's lives and reducing mortality rates. The scalability of IoMT enables a significant number of patients to be remotely monitored from their homes or hospitals without the need for in-person visits. As indicated by All the Research, the global COVID-19 pandemic has accelerated the adoption of IoMT and has become instrumental in advancing the development of this technology.

The IoMT ecosystem is strengthened by various technologies such as Wireless Sensor Networks (WSN), Bluetooth, ZigBee, WiFi, NB-IoT, LTE, 4G, and 5G, in combination with big data analytics, Artificial Intelligence (AI), and cloud computing. This convergence of technologies forms a powerful health-tech ecosystem that enables efficient data transmission, advanced analytics, and improved decision-making in healthcare settings [32].

In summary, the deployment of IoMT brings numerous advantages to the healthcare industry, including reduced errors, accurate disease diagnosis, cost savings, and enhanced remote communication between patients and doctors. It has demonstrated substantial outcomes in terms of financial savings, reduced hospital admission times, shorter treatment stays, minimized procedure cancellations, and decreased staff overtime. In addition, IoMT has played a vital role in combatting the COVID-19 pandemic by providing protection for healthcare workers, increasing productivity, reducing the burden on individuals' lives, and lowering mortality rates. The accelerated adoption of IoMT during this global crisis has further propelled its development, aided by the integration of various technologies and the establishment of a robust health-tech ecosystem.

### THE NEED FOR INTEGRITY AND SAFETY IN THE IOMT SYSTEM

The widespread adoption of IoMT (Internet of Medical Things) has significantly increased the vulnerability of the data handled within its environment, making it more susceptible to cyber attacks. In the unfortunate event that an attacker with malicious intent gains unauthorized access to the IoMT system, the consequences can be severe, endangering not only the sensitive user data but also the lives of patients in certain situations. Extensive research and collaboration within the community have led to the identification of numerous vulnerabilities present in IoMT environments.

This section aims to address some of the prevalent vulnerabilities that exist within IoMT environments and highlight the legal frameworks established to protect against these weaknesses. As IoMT systems involve the transmission and storage of sensitive medical data, they become attractive targets for attackers seeking to exploit vulnerabilities and gain unauthorized access. The potential consequences of such breaches are far-reaching, ranging from privacy breaches to unauthorized tampering with medical devices, which can pose serious risks to patient safety and well-being.

To mitigate these vulnerabilities, both technical and regulatory measures have been implemented. Technical solutions involve the adoption of robust security protocols, encryption mechanisms, and access controls to safeguard data and prevent unauthorized access. Furthermore, regular system monitoring, vulnerability assessments, and incident response plans are essential to proactively identify and address potential threats.

In terms of regulatory frameworks, various laws and regulations are in place to protect the security and privacy of medical data within IoMT environments. These regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in the European Union, and other country-specific data protection laws, impose obligations on healthcare organizations and technology providers to implement appropriate security measures, ensure data privacy, and establish breach notification protocols.

Additionally, collaboration within the IoMT community is crucial in identifying and addressing vulnerabilities. Researchers, industry experts, and regulatory bodies work together to share knowledge, conduct audits, and develop best practices for securing IoMT systems. This collaborative effort plays a significant role in continuously improving the security posture of IoMT environments and staying ahead of emerging threats.

In conclusion, the broad adoption of IoMT has heightened the vulnerability of the data handled within its environment. However, through research, collaboration, and the implementation of technical measures and regulatory frameworks, efforts are being made to address the prevalent vulnerabilities and enhance the security of IoMT systems. It is essential to remain vigilant, regularly assess risks, and adhere to established guidelines to protect sensitive data and ensure the safety of patients in the evolving landscape of IoMT.

### IV. I SECURITY INCIDENTS AT THE IOMT

Preserving the confidentiality and privacy of patients' information is of paramount importance in establishing a trustworthy healthcare system that delivers exceptional care. The healthcare sector, unlike other systems, holds a unique position as people's lives and well-being depend on it. Ensuring the security of computing systems is vital, encompassing the protection of hardware, software, and data, which collectively form the CIA trinity. Information security revolves around three fundamental tenets: (1) secrecy, maintaining the confidentiality of data; (2) prevention of unauthorized access and maintaining the integrity of data resources; and (3) availability, ensuring continuous access to data. Unfortunately, IoMT has witnessed numerous security breaches, reflecting the continuous efforts of criminals to infiltrate corporate networks, steal sensitive information, manipulate existing files, or exploit employees for blackmail purposes.

Throughout January 2018, approximately 115 cyberattacks were reported, with over 2.9 million subscribers of Health South-East RHF being affected by one such incident. The infamous WannaCry ransomware attack on England's National Health Service (NHS) stands out as one of the most severe and devastating breaches in the healthcare sector. This attack led to the cancellation of 19,000 appointments and incurred GBP 92 million in costs for mitigation and recovery [33]. Disturbingly, nearly 90% of healthcare companies utilizing IoMT have experienced at least one security compromise. In 2016, a comprehensive analysis revealed that 370 IoMT businesses, accounting for 35% of all businesses, encountered at least one cybersecurity breach. Ransomware assaults specifically targeted IoMT in 45% of all incidents reported in 2017. The MEDJACK 2 case exemplified how ransomware attacks could successfully infiltrate IoMT environments, resulting in data theft. The largest ransomware attack recorded in 2017 affected over 200,000 devices worldwide [34].

In December 2020, a healthcare cybersecurity vendor, CyberMDX, discovered an authentication vulnerability in multiple GE Healthcare machines. This discovery prompted the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency to issue an advisory to hospitals and medical organizations, emphasizing the potential threat to protected health information. The severity level of the vulnerability was classified as 9.8. Furthermore, a recent alert revealed potential interference with clinical data by MedTronic MyCareLink (MCL) Medical Devices (MDs). Vulnerabilities were identified in all versions of the MCL Smart Model 25000 Patient Reader.

Forescout Research Labs also discovered 33 vulnerabilities in four open-source TCP/IP stacks that could potentially impact 150 enterprises and millions of MDs. These vulnerabilities, known as AMNESIA:33, affect DNS, IPv6, and TCP protocols [35]. Notably, an Indiana hospital incurred a cost of $50,000 in 2018 to restore its data following a cyberattack. Figure 6 showcases MD manufacturers who acknowledged experiencing cyberattacks on their products in the year prior to the Irdeto 2019 survey [36].

These instances underscore the urgent need for robust security measures within IoMT environments. The vulnerabilities and breaches highlighted demonstrate the ever-present risks faced by the healthcare sector in ensuring the privacy and security of patient data. Vigilance and proactive measures must be taken to safeguard against such threats, providing a secure foundation for the advancement and widespread adoption of IoMT technologies.

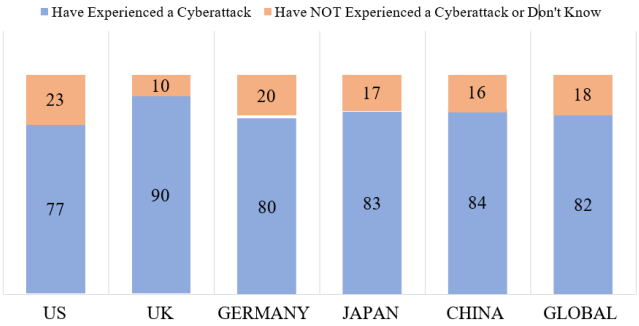


**Figure 9: 2019 Irdeto survey.**

### IV. GUIDELINES FOR CYBERSECURITY IN THE IOMT

Regulatory agencies are taking proactive measures to address the potential safety hazards associated with medical devices (MDs) by revising pre-market cybersecurity regulations. One of the key governing bodies overseeing the MD market is the Food and Drug Administration (FDA), which closely monitors security issues pertaining to MDs in order to ensure patient safety. In October 2014, the FDA issued the Premarket Submissions for Cybersecurity Management guidelines, aimed at providing recommendations and standards for enhancing security management and reducing risks associated with MD operations. These guidelines have prompted MD manufacturers to incorporate specific design and development criteria to prevent cybersecurity issues.

To adhere to the FDA guidelines, MD manufacturers are required to establish a robust cybersecurity vulnerability and management methodology as part of their software validation and risk assessment processes. Furthermore, the FDA's draft recommendation on postmarket management in 2016 [37]

proposed the implementation of a comprehensive cybersecurity risk-management program throughout the entire lifecycle of MDs, encompassing both the pre-market and post-market stages. This holistic approach ensures that cybersecurity concerns are addressed at all stages of the device's lifespan.

In line with these efforts, in 2018, a new category of pre-market guidance was proposed for connected Tier 1 and Tier 2 MDs, with the intention of soliciting public feedback. This proposed guidance aims to provide specific guidelines and requirements for MD manufacturers to follow, focusing on the cybersecurity aspects of connected devices.

By revising pre-market cybersecurity rules and establishing comprehensive guidelines, regulatory agencies are proactively addressing the potential risks associated with MD security. These measures are designed to ensure that MD manufacturers integrate robust cybersecurity practices into their design, development, and post-market management processes. Through such initiatives, governing agencies aim to enhance user and patient safety in the rapidly evolving landscape of medical device technology.


**Figure 10: Advances in the cybersecurity regulations for medical devices.**

## V. SAFEGUARDING SYSTEMS

In IoT environments, two primary types of security measures are commonly employed: software-based and hardware-based solutions. Software-based security solutions rely on mathematical techniques to safeguard computer systems. While current mathematical methods may take time to solve, the emergence of quantum computers is expected to significantly accelerate key extraction processes.

On the other hand, hardware-based security solutions utilize encryption algorithms such as KPI (Key Performance Indicator), AES (Advanced Encryption Standard), and ECC (Elliptic Curve Cryptography). Shared-key configurations with the server or other devices are typically employed in KPI-based solutions. Although KPI offers advantages in terms of low computing complexity and high efficiency, it becomes impractical when dealing with a large number of devices. In contrast, asymmetric protocols eliminate the need for pre-shared parameter keys. These protocols utilize both public and private keys, ensuring privacy through the use of secret keys [38]. In dense device environments, the major challenges in establishing secure communication for IoT lie in device authentication and key exchange. Moreover, these IoT devices often have limited processing speed, energy resources, and storage capacity.

To address these challenges, researchers are actively working on developing authentication mechanisms. Among various authentication systems, Physically Unclonable Functions (PUFs) stand out due to their low power consumption and fast verification of user legitimacy. In the context of IoMT, PUFs provide a digitally unique fingerprint that serves as a physically defined security primitive. A PUF is a tangible entity that offers a distinctive response to a specific query or challenge. Leveraging the inherent physical diversity of integrated circuits, PUFs serve as a challenge-response mechanism in security contexts [39]. The unpredictable and uncontrollable side effects of the integrated circuit manufacturing process make each PUF unique and non-replicable. For user authentication, PUFs generate a unique challenge-response pair (CPR) upon request.

In summary, IoT environments employ software-based and hardware-based security measures. Software-based solutions utilize mathematical techniques, while hardware-based solutions utilize encryption algorithms like KPI, AES, and ECC. Device authentication and key exchange pose significant challenges in secure communication for IoT, especially in device-dense settings. PUFs, with their low power consumption and unique challenge-response capability, offer a promising authentication mechanism in the context of IoMT. The inherent physical diversity of PUFs ensures their non-replicability, providing a robust security primitive for user authentication.

## VI. PROTECTION MEASURES FOR THE INTERNET OF THINGS

This section provides a literature review on existing security solutions for the IoMT network. The following studies are discussed, outlining their contributions, limitations, and improvements:

Chiou et al. [40] proposed an authentication technique for IoMT in 2016. However, Deebak et al. [41] identified limitations in Chiou et al.'s solution, specifically in terms of comprehensive protection against security attacks and patient identity concealment. Both studies utilized secret keys for user authentication, but Chiou et al. transmitted the secret key over a public channel, while Deebak et al. encrypted it with other parameters. Although Deebak et al. made improvements to the authentication process, limitations identified in Chiou et al.'s approach remained unresolved.

Park et al. [42] examined Xu et al.'s system [43] and identified vulnerabilities related to impersonation, stolen sensor nodes, and leaking verification table attacks. Xu et al.'s system did not provide sufficient privacy, invisibility, or trustworthiness for its users. Park et al. addressed these challenges by not storing client authentication parameters or sensitive data on the server. However, a potential single point of failure could

occur during registration when an intermediate node is assigned for the sensor-to-server connection. Park et al. proposed a lightweight authentication system that combines XOR and hash algorithms to generate a session key.

Chen et al. [44] introduced a group-oriented time-bound authenticated key agreement using chaotic maps [45]. Chaotic maps were chosen for their large parameter space, uniform data distribution, and semigroup structure. In this approach, permitted entities can utilize a group key for a limited time before a new key is generated. The server transmits an authentication window and available time to service providers and user groups. If the application provider receives a matching token within the time limit, authentication is successful. However, it is unclear how a group's shared authentication token will be distributed among its members.

Li et al. [46] proposed a lightweight approach using Hash and XOR algorithms. Their solution involved six steps utilizing open channels. Prior to deployment, a sensor and trusted gateway share a secure key. Users and sensor nodes can join the gateway registration process using this private key. With the assistance of the gateway, the sensor and user negotiate a session key for encrypting sensor data.

In summary, the reviewed literature presents various security solutions for the IoMT network. While each approach offers unique contributions, they also exhibit limitations that need to be addressed. These studies provide valuable insights for further research and development, highlighting the importance of improving authentication methods, addressing vulnerabilities, ensuring privacy, and establishing secure communication channels within the IoMT network

### VI.I. ATTRIBUTE BASED

Zhang et al. [47] introduced an attribute-based encryption (ABE) authentication mechanism that requires both centralised and attribute authorities. Users wishing to authenticate with the cloud must send a signed secret key and transformation key to the cloud user assistant.

However, ABE-based systems face certain challenges. Firstly, it is difficult to determine who is using a secret key or detect unauthorized distribution of keys. Secondly, as the number of attributes increases, the size of ciphertext also grows, resulting in longer decryption times [48]. Furthermore, ABE can be computationally expensive for lightweight devices, making decryption impractical [49].

In response to these challenges, Liu et al. [50] proposed a solution that connects wearables to a hospital-based edge computing server. The client and server generate pseudo-numbers and compute data attributes using numbers and secret keys to authenticate. To facilitate computations and transmission, the secret key is partitioned into multiple pieces. This approach aims to minimize data processing and storage requirements for IoT devices. However, similar to Kumar et al., not all types of attacks (such as Denial of Service and reply attacks) were fully addressed. To address these limitations, Hwang et al. [48] proposed ciphertext-policy attribute-based authentication (CP-ABE).

CP-ABE relies on a combination of trusted authority and attribute authority to determine the first key issuer. When the number of attributes is fixed, the decryption time remains independent of the number of attributes due to the constant ciphertext size. However, the suggested approach requires significant computational resources for identity verification. Additionally, there is a risk of confidential information leakage by the recipient of the delegated key.

In summary, Zhang et al. presented an ABE authentication mechanism, highlighting the challenges associated with ABE-based systems, including key distribution and ciphertext size. Liu et al. proposed an approach that connects wearables to an edge computing server, while Hwang et al. introduced CP-ABE to address certain limitations of attribute-based authentication. These studies shed light on the potential of different authentication mechanisms in the context of the IoT, emphasizing the need for further research to overcome the computational challenges and ensure robust security in IoMT environments.

### VI. II ANALYZING HEART RATE VIA ELECTROCARDIOGRAM

Huang et al. [51] proposed an ECG-based authentication scheme using singular value decomposition (SVD) to denoise electrocardiogram (ECG) signals. The objective of this scheme was to reduce background noise in ECG signals by employing motion detection and standard feature templates. Through the utilization of weighted online SVD, a denoised signal was generated for cases involving mild activity.

However, the scheme faced challenges in obtaining accurate angular distance measurements for activities such as walking and running, as well as for various other workout scenarios. The authors assumed that intruders would not have access to ECG templates from the patients involved in their study. Nevertheless, the scheme lacked adequate protection for user identities, and the computational time required was found to be excessive.

In summary, Huang et al. developed an ECG-based authentication scheme utilizing SVD for denoising ECG signals. While the scheme showed promise in reducing background noise and generating denoised signals, challenges remained in accurately measuring angular distances for different activities. Additionally, the scheme's lack of robust user identity protection and excessive computational time raised concerns. Further research and improvements are necessary to enhance the accuracy and security of ECG-based authentication systems in the context of IoMT.

### VI.III MAC-BASED SYSTEM REQUIREMENT

Xu et al. [9] proposed a data collection system for medical devices (MDs) where a gateway collects data from the devices and stores it in the cloud using a MAC (Message Authentication Code) protocol. The data can be encrypted

using information shared in advance with a trusted party, ensuring authentication and data protection. However, the study highlighted the lack of security in data transfer between IoT devices and the gateway, emphasizing the need for a secure channel to transmit the computed key to the IoT gateway.

In the context of smart cards and MDs, a suggested authentication methodology utilizes public-key cryptography and verifies user IDs using MAC addresses. The server supplies a hash function with a missing k-bit, and the reader device must calculate and identify it for authentication. However, this proposed protocol lacks user privacy, as the authentication process reveals sensitive information.

Hahn et al. [49] developed a mechanism involving a key server that generates both a verification key and a commitment key. With these keys, users can evaluate their dedication and share the results. A doctor can verify the commitment key using the provided verification key and commitment key.

In summary, Xu et al. proposed a data collection system for MDs with a MAC protocol to ensure authentication and secure data transfer. However, the study emphasized the need for improved security in data transfer between IoT devices and the gateway. The suggested authentication methodology for smart cards and MDs relied on public-key cryptography but lacked user privacy. Hahn et al. introduced a mechanism involving key generation and verification for evaluating dedication and ensuring data integrity. Further research is necessary to address the security and privacy concerns raised in these authentication protocols for IoT and MD environments.

## VI. IV ML-BASED SYSTEM REQUIREMENT

In their work, Wang et al. [52] presented a privacy-protecting outsourced support vector machine (SVM) and proposed the utilization of eight privacy-preserving outsourced computation techniques. The objective of their protocol was to outsource both integer and floating-point computations to enhance computational efficiency and ensure correctness. To achieve secure and private processing, the floating-point numbers were normalized using 2E fixed-point precision. The protocol involved a trusted third party responsible for distributing a public-private key pair to all users, after which it remained inactive. Notably, the cloud service provider and server held the private keys.

The primary focus of the protocol was to safeguard user privacy while facilitating computations in an outsourced environment. By outsourcing the computation tasks, users could benefit from the computational resources and capabilities offered by the cloud service provider without compromising the confidentiality of their data. The protocol incorporated various privacy-preserving techniques to protect sensitive information during the computation process.

Efficiency and correctness were key considerations in the protocol design. Integer and floating-point computations were effectively delegated to the cloud service provider to optimize computational performance. The use of fixed-point precision for normalizing floating-point numbers ensured consistency and accuracy in the computation results. Furthermore, the distribution of public-private key pairs by the trusted third party and the possession of private keys by the cloud service provider and server contributed to the secure execution of the protocol.

In summary, Wang et al. proposed a privacy-protecting outsourced support vector machine that employed a set of privacy-preserving outsourced computation techniques. The protocol aimed to safeguard user privacy while outsourcing computation tasks to a cloud service provider. By leveraging the techniques discussed, the protocol achieved efficient and correct computations while maintaining the security and privacy of user data. Further research is warranted to explore the practical implementation and scalability of such privacy-preserving protocols in real-world scenarios involving IoT and cloud computing environments.

## VII. BLOCK CHAIN BASED

Abdellatif et al. [53] propose a holistic framework that integrates edge computing and blockchain technology for processing medical data. The framework includes an automatic patient-monitoring strategy and a blockchain system with three distinct channels to segregate urgent data. To minimize latency and ensure timely response, the urgent data is given top priority and is processed using a less-restrictive blockchain configuration. The focus of this work lies in defining priorities and extracting relevant features from the medical data.

The proposed blockchain technology, named Healthchain, employs a proof-of-work mechanism and encryption techniques to secure health data and enforce access control. Healthchain comprises two main components: Userchain and Docchain. IoT data is encrypted using symmetric AES encryption, and the accounting nodes in Docchain, acting as miners, add data from doctor nodes to the blockchain. In the event of a compromised IoT key or diagnosis key, the user can initiate a fresh key transaction to ensure data security.

Hashing is performed using SHA-256, while asymmetric encryption and signing utilize 1024-bit RSA. This approach provides conditional security by safeguarding the private keys of both patients and doctors and limiting the computational power available to adversaries. Detection of fraudulent transactions and nodes necessitates a third-party audit.

The proposed framework offers a comprehensive solution for secure and efficient processing of medical data by leveraging the combined benefits of edge computing and blockchain technology. By prioritizing urgent data and employing encryption and access control mechanisms, the framework ensures the integrity and confidentiality of medical information. However, further research and evaluation are required to assess the scalability, performance, and practicality of the proposed framework in real-world healthcare

environments. Additionally, considerations regarding regulatory compliance, interoperability, and the integration of existing healthcare systems should be explored.

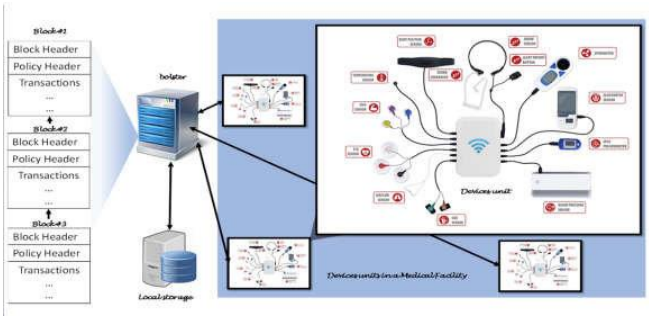


**Figure 11: Introduction to the structure of the blockchain-based IoMT system [57]**

## VIII. CONCLUSION

The continuous expansion of internet-connected devices in the Internet of Medical Things (IoMT) has raised concerns about potential security vulnerabilities within these systems. Ensuring the security of IoMT systems requires ongoing efforts by researchers and industry experts to identify and rectify weaknesses that could be exploited by malicious actors. Various approaches and techniques are being developed to address these security challenges. It is essential to establish a universal standard that manufacturers adhere to in order to ensure the security and consistency of the IoT ecosystem. Regulatory organizations, such as the Food and Drug Administration (FDA) and the European Union (EU), are actively involved in developing and revising regulations to address these gaps, and compliance with these regulations is mandatory for manufacturers to bring their products to market. This study aims to provide a comprehensive examination of the IoT ecosystem, its roles, and the associated risks.

The research conducted in this study encompasses an extensive exploration of existing IoT security techniques with the goal of enhancing security and privacy. Various authentication technologies, including Attribute-Based Encryption (ABE), Elliptic Curve Cryptography (ECC), Message Authentication Codes (MAC), Machine Learning (ML), Physical Unclonable Functions (PUF), and Blockchain, are compared to assess their efficacy. The implementation described in this study utilizes Named Data Networking (NDN) technology, which is undergoing continuous refinement. The study also addresses critical barriers to the integration of Internet of Medical Things (IoMT) systems, such as scalability, memory requirements, computing resources, communication overhead, energy efficiency, and security considerations.

Future research endeavors will delve into the possibilities and implications of post-quantum and post-5G technologies in the context of IoMT. These advancements will be explored to identify potential benefits and challenges they may introduce. The study will also address prevailing security issues, such as the vulnerability identified in June 2022 that allows for remote exploitation of cryptographic keys in CPUs manufactured by Intel, AMD, and other vendors. An investigation into the causes of these flaws and potential remedies will be conducted to enhance the security posture of IoMT systems.

In conclusion, securing IoT systems against potential vulnerabilities is of paramount importance as the number of internet-connected devices continues to grow exponentially. The establishment of a universal standard and the enactment of robust regulatory frameworks are key factors in ensuring the security and consistency of the IoT ecosystem. Through a comprehensive analysis of existing IoT security techniques and exploration of emerging technologies, this study contributes to ongoing efforts to enhance the security and privacy of IoMT systems. Future research endeavors will build upon these findings, exploring advanced post-quantum and post-5G possibilities, addressing prevailing security issues, and investigating causes and remedies for identified flaws.

## REFERENCES

[1]. Tran-Dang, H.; Krommenacker, N.; Charpentier, P.; Kim, D.S. Toward the Internet of Things for Physical Internet: Perspectives and Challenges. IEEE Internet Things J. 2020, 7, 4711–4736

[2]. Wazid, M.; Singh, J.; Das, A.K.; Shetty, S.; Khan, M.K.; Rodrigues, J.J.P.C. ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things. IEEE Access 2022, 10, 57990–58004

[3]. Amin, F.; Majeed, A.; Mateen, A.; Abbasi, R.; Hwang, S.O. A Systematic Survey on the Recent Advancements in the Social Internet of Things. IEEE Access 2022, 10, 63867–63884

[4]. Sadhu, P.; Yanambaka, V.P.; Abdelgawad, A.; Yelamarthi, K. NAHAP: PUF-Based Three Factor Authentication System for Internet of Medical Things. IEEE Consum. Electron. Mag. 2022

[5]. Internet of Medical Things Market. Available online: https://www2.deloitte.com/ie/en/pages/life-sciences-and-healthcare/ articles/internet-of-medical-things.html

[6]. . Internet of Medical Things Revolutionizing Healthcare. Available online: https://aabme.asme.org/posts/internet-of-medical- things-revolutionizing-healthcare/

[7]. Alamri, B.; Crowley, K.; Richardson, I. Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review. IEEE Access 2022, 10, 59612–59629

[8]. Aledhari, M.; Razzak, R.; Qolomany, B.; Al-Fuqaha, A.; Saeed, F. Biomedical IoT: Enabling Technologies, Architectural Elements, Challenges, and Future Directions. IEEE Access 2022, 10, 31306–31339

[9]. Xu, C.; Wang, N.; Zhu, L.; Sharif, K.; Zhang, C. Achieving Searchable and Privacy-preserving Data Sharing for Cloud-assisted E-healthcare System. IEEE Internet Things J. 2019, 6, 8345–8356

[10]. Hernandez, S.; Raison, M.; Torres, A.; Gaudet, G.; Achiche, S. From on-body Sensors to in-body Data for Health Monitoring and Medical Robotics: A Survey. In Proceedings of the Global Information Infrastructure and Networking Symposium (GIIS), Montreal, QC, Canada, 15–19 September 2014; pp. 1–5

[11]. Noguchi, H.; Mori, T.; Sato, T. Framework for Search Application based on Time Segment of Sensor Data in Home Environment. In Proceedings of the Seventh International

Conference on Networked Sensing Systems (INSS), Kassel, Germany, 15–18 June 2010; pp. 261–264

[12]. Internet of Medical Things (IoMT) Market By Component, Platform, Connectivity Devices, Application and Is Expected to Reach USD 1,84,592.31 Million by 2028. Available online: https://www.marketwatch.com/press-release/internet-of-medical-things- iomt-market-by-component-platform-connectivity-devices-application-and-is-expected-to-reach-usd-18459231-million-by-20 28-2022-04-26

[13]. What Is the Internet of Medical Things (IoMT)? Available online: https://mobius.md/2019/03/06/what-is-the-iomt/ (accessed on 22 June 2022)

[14]. Masud, M.; Gaba, G.S.; Alqahtani, S.; Muhammad, G.; Gupta, B.B.; Kumar, P.; Ghoneim, A. A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care. IEEE Internet Things J. 2021, 8, 15694–15703

[15]. Saheed, Y.K.; Arowolo, M.O. Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms. IEEE Access 2021, 9, 161546–161554

[16]. Hameed, K.; Garg, S.; Amin, M.B.; Kang, B.; Khan, A. A Context-aware Information-based Clone Node Attack Detection Scheme in Internet of Things. J. Netw. Comput. Appl. 2022, 197, 103271

[17]. Sengupta, J.; Ruj, S.; Bit, S.D. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. J. Netw. Comput. Appl. 2020, 149, 102481

[18]. Shamsoshoara, A.; Korenda, A.; Afghah, F.; Zeadally, S. A Survey on Physical Unclonable Function (PUF)-based Security Solutions for Internet of Things. Comput. Netw. 2020, 183, 107593

[19]. Fernández-Caramés, T.M. From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. IEEE Internet Things J. 2020, 7, 6457–6480

[20]. Alwarafy, A.; Al-Thelaya, K.A.; Abdallah, M.; Schneider, J.; Hamdi, M. A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things. IEEE Internet Things J. 2021, 8, 4004–4022

[21]. Shakeel, T.; Habib, S.; Boulila, W.; Koubaa, A.; Javed, A.R.; Rizwan, M.; Gadekallu, T.R.; Sufiyan, M. A Survey on COVID-19 Impact in the Healthcare Domain: Worldwide Market Implementation, Applications, Security and Privacy Issues, Challenges and Future Prospects. Complex Intell. Syst. 2022, 1–32

[22]. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Commun. Surv. Tutor. 2020, 22, 1646–1685

[23]. Arora, P.; Kaur, B.; Teixeira, M.A. Machine Learning-Based Security Solutions for Healthcare: An Overview. Emerg. Technol. Comput. Commun. Smart Cities 2022, 649–659

[24]. Rbah, Y.; Mahfoudi, M.; Balboul, Y.; Fattah, M.; Mazer, S.; Elbekkali, M.; Bernoussi, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems in IoMT: A survey. In Proceedings of the 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Meknes, Morocco, 3–4 March 2022; pp. 1–9

[25]. Sadawi, A.A.; Hassan, M.S.; Ndiaye, M. A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges. IEEE Access 2021, 9, 54478–54497

[26]. Khor, J.H.; Sidorov, M.; Woon, P.Y. Public Blockchains for Resource-Constrained IoT Devices—A State-of-the-Art Survey. IEEE Internet Things J. 2021, 8, 11960–11982

[27]. Awad, A.; Fouda, M.M.; Khashaba, M.M.; Mohamed, E.R.; Hosny, K.M. Utilization of mobile edge computing on the Internet of Medical Things: A survey. ICT Express 2022

[28]. Global Internet of Medical Things (IoMT) Market. Available online: https://www.alltheresearch.com/report/166/internet-ofmedical-things-market

[29]. Afroz, M., ; Goswami, B. (2022). “A vulnerability to storage security for cloud computing”. Lecture Notes in Networks and Systems. In-press. https://doi.org/Congress on Intelligent Systems

[30]. How Connected Medical Devices Are Transforming Health Care. Available online: https://www2.deloitte.com/global/en/

[31]. 5 Reasons IoMT Devices Make Sense for Healthcare Organizations. Available online: https://healthtechmagazine.net/article/2020/04/5-reasons-iomt-devices-make-sense-healthcare-organizations/

[32]. Aman, A.H.M.; Hassan, W.H.; Sameen, S.; Attarbashi, Z.S.; Alizadeh, M.; Latiff, L.A. IoMT Amid COVID-19 Pandemic: Application, Architecture, Technology, and Security. J. Netw. Comput. Appl. 2020, 174, 102886

[33]. Jahankhani, H.; Ibarra, J. Digital Forensic Investigation for the Internet of Medical Things (IoMT). Forensic Leg. Investig. Sci. 2019,5, 29

[34]. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of Medical Things Security Assessment Framework.Internet Things 2019, 8, 100123.

[35]. Medical Device Security. Available online: https://healthitsecurity.com/tag/medical-device-security/

[36]. Medical Device Cybersecurity in the Age of IoMT. Available online: https://www.medtechintelligence.com/column/medicaldevice-cybersecurity-in-the-age-of-iomt/

[37]. Wu, L.; Du, X.; Guizani, M.; Mohamed, A. Access Control Schemes for Implantable Medical Devices: A Survey. IEEE Internet Things J. 2017, 4, 1272–1283

[38]. Li, S.; Zhang, T.; Yu, B.; He, K. A Provably Secure and Practical PUF-based End-to-End Mutual Authentication and Key Exchange Protocol for IoT. IEEE Sensors J. 2020, 21, 5487–5501

[39]. Aman, M.N.; Javaid, U.; Sikdar, B. A Privacy-preserving and Scalable Authentication Protocol for the Internet of Vehicles. IEEE Internet Things J. 2020, 8, 1123–1139

[40]. Chiou, S.Y.; Ying, Z.; Liu, J. Improvement of a Privacy Authentication Scheme Based on Cloud for Medical Environment. J. Med. Syst. 2016, 40, 10

[41]. Deebak, B.D.; Al-Turjman, F. Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems using Internet of Medical Things. IEEE J. Sel. Areas Commun. 2020, 39, 346–360

[42]. Park, K.; Noh, S.; Lee, H.; Das, A.K.; Kim, M.; Park, Y.; Wazid, M. LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme without Verification

Table in Medical Internet of Things. IEEE Access 2020, 8, 119387–119404

[43]. Xu, Z.; Xu, C.; Liang, W.; Xu, J.; Chen, H. A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things. IEEE Access 2019, 7, 53922–53931

[44]. Chen, M.; Lee, T.F. Anonymous Group-oriented Time-bound Key Agreement for Internet of Medical Things in Telemonitoring Using Chaotic-maps. IEEE Internet Things J. 2021, 8, 13939–13949

[45]. Dharminder, D.; Gupta, P. Security Analysis and Application of Chebyshev Chaotic Map in the Authentication Protocols. Int. J. Comput. Appl. 2019, 43, 1095–1103

[46]. Li, J.; Su, Z.; Guo, D.; Choo, K.K.R.; Ji, Y. PSL-MAAKA: Provably-Secure and Lightweight Mutual Authentication and Key Agreement Protocol for Fully Public Channels in Internet of Medical Things. IEEE Internet Things J. 2021, 8, 13183–13195

[47]. Zhang, L.; Ye, Y.; Mu, Y. Multiauthority Access Control With Anonymous Authentication for Personal Health Record. IEEE Internet Things J. 2020, 8, 156–167

[48]. Hwang, Y.W.; Lee, I.Y. A Study on CP-ABE-Based Medical Data Sharing System with Key Abuse Prevention and Verifiable Outsourcing in the IoMT Environment. Sensors 2020, 20, 4934

[49]. Hahn, C.; Kwon, H.; Hur, J. Trustworthy Delegation Toward Securing Mobile Healthcare Cyber-physical Systems. IEEE Internet Things J. 2018, 6, 6301–6309

[50]. Liu, H.; Yao, X.; Yang, T.; Ning, H. Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing-based Smart Health. IEEE Internet Things J. 2018, 6, 1352–1362

[51]. Huang, P.; Guo, L.; Li, M.; Fang, Y. Practical Privacy-preserving ECG-based Authentication for IoT-based Healthcare. IEEE Internet Things J. 2019, 6, 9200–9210

[52]. Wang, J.; Wu, L.; Wang, H.; Choo, K.K.R.; He, D. An Efficient and Privacy-Preserving Outsourced Support Vector Machine Training for Internet of Medical Things. IEEE Internet Things J. 2020, 8, 458–473

[53]. Abdellatif, A.A.; Samara, L.; Mohamed, A.; Erbad, A.; Chiasserini, C.F.; Guizani, M.; O'Connor, M.D.; Laughton, J. Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange. IEEE Internet Things J. 2021, 8, 15762–15775

[54]. Ovunc Kocabas, Tolga Soyata, and Mehmet K Aktas. Emerging security mechanisms for medical cyber physical systems. IEEE/ACM transactions on computational biology and bioinformatics, 13(3):401416, 2016

[55]. Carmen CY Poon, Yuan-Ting Zhang, and Shu-Di Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Communications Magazine, 44(4):73–81, 2006

[56]. Krishna K Venkatasubramanian, Ayan Banerjee, and Sandeep Kumar S Gupta. Pska: Usable and secure key agreement scheme for body area networks. IEEE Transactions on Information Technology in Biomedicine, 14(1):60–68, 2010

[57]. Seliem, Mohamed & Elgazzar, Khalid. (2019). BIoMT: Blockchain for the Internet of Medical Things. 10.1109/BlackSeaCom.2019.8812784.